Offshore wind farms are vulnerable to cyberattacks, study shows

January 24 2024, by Patrick Lejtenyi

Credit: Unsplash/CC0 Public Domain

The hurrying pace of societal electrification is encouraging from a climate perspective. But the transition away from fossil fuels toward renewable sources like wind presents new risks that are not yet fully understood.

Researchers from Concordia and Hydro-Quebec presented a new study on the topic in Glasgow, United Kingdom at the 2023 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm). Their study explores the risks of cyberattacks faced by offshore wind farms. Specifically, the researchers considered wind farms that use voltage-source-converter high-voltage direct-current (VSC-HVDC) connections, which are rapidly becoming the most cost-effective solution to harvest offshore wind energy around the world.

"As we advance the integration of renewable energies, it is imperative to recognize that we are venturing into uncharted territory, with unknown vulnerabilities and cyber threats," says Juanwei Chen, a Ph.D. student at the Concordia Institute for Information Systems Engineering (CIISE) at the Gina Cody School of Engineering and Computer Science.

"Offshore wind farms are connected to the main power grid using HVDC technologies. These farms may face new operational challenges," Chen explains. "Our focus is to investigate how these challenges could be intensified by cyber threats and to assess the broader impact these threats might have on our power grid."

Concordia Ph.D. student Hang Du, CIISE associate professor Jun Yan and Gina Cody School dean Mourad Debbabi, along with Rawad Zgheib from the Hydro-Quebec Research Institute (IREQ), also contributed to the study. This work is part of a broad research collaboration project involving the group of Prof. Debbabi and the IREQ cybersecurity research group led by Dr. Marthe Kassouf and involving a team of researchers including Dr. Zgheib.

Complex and vulnerable systems

Offshore wind farms require more cyber infrastructure than onshore

wind farms, given that offshore farms are often dozens of kilometers from land and are operated remotely. Offshore wind farms need to communicate with onshore systems via a wide area network. Meanwhile, the turbines also communicate with maintenance vessels and inspection drones, as well as with each other.

This complex, hybrid-communication architecture presents multiple access points for cyberattacks. If malicious actors were able to penetrate the local area network of the converter station on the wind farm side, these actors could tamper with the system's sensors. This tampering could lead to the replacement of actual data with false information. As a result, electrical disturbances would affect the offshore wind farm at the points of common coupling.

In turn, these disturbances could trigger poorly dampened power oscillations from the offshore wind farms when all the offshore wind farms are generating their maximum output. If these cyber-induced electrical disturbances are repetitive and match the frequency of the poorly dampened power oscillations, the oscillations could be amplified.

These amplified oscillations might then be transmitted through the HVDC system, potentially reaching and affecting the stability of the main power grid. While existing systems usually have redundancies built in to protect them against physical contingencies, such protection is rare against cyber security breaches.

"The system networks can handle events like router failures or signal decays. If there is an attacker in the middle who is trying to hijack the signals, then that becomes more concerning," says Yan, the Concordia University Research Chair (Tier 2) in Artificial Intelligence in Cyber Security and Resilience.

Yan adds that considerable gaps exist in the industry, both among

manufacturers and utilities. While many organizations are focusing on corporate issues such as data security and access controls, much is to be done to strengthen the security of operational technologies.

He notes that Concordia is leading the push for international standardization efforts but acknowledges the work is just beginning.

"There are regulatory standards for the US and Canada, but they often only state what is required without specifying how it should be done," he says. "Researchers and operators are aware of the need to protect our energy security, but there remain many directions to pursue and open questions to answer."

More information: Juanwei Chen et al, A Data Integrity Attack Targeting VSC-HVDC-Connected Offshore Wind Farms, *2023 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)* (2023). DOI: 10.1109/SmartGridComm57358.2023.10333872

Provided by Concordia University